CLAIMS

What is claimed is:

1. A computing system comprising:

a processor and chipset to provide for protected execution of code;

a hardware token including a credential data store; and

a storage device storing code to implement Subscriber Identity Module (SIM) algorithms, the SIM algorithms to be executed by the processor in a protected partition.

2. The computing system of claim 1 wherein,

the hardware token is a Trusted Platform Module (TPM).

3. The computing system of claim 1 wherein,

the processor is a microprocessor, and

the computing system is a notebook computer system.

4. The computing system of claim 3 wherein,

the storage device is one of a hard disk and a compact disc.

5, The computing system of claim 3 wherein,

the storage device further stores a provisioning algorithm to provide for provisioning of SIM secret data objects.

6. The computing system of claim 1 wherein,

the computing system executes an operating system that provides for protected software execution.

7. The computing system of claim 1 wherein,

the SIM algorithms include code to execute one or more of a set of algorithms including an authentication algorithm, a cipher key generator algorithm, an encryption algorithm and a decryption algorithm.

8. The computing system of claim 7 wherein,

the set of algorithms includes A3, A8 and A5 algorithms.

9. A computing system comprising:

a battery connector to receive a battery to provide an alternate power source for the computing system;

a wireless module to provide for wireless communications;

a processor to provide for protected execution of code; and

a data store storing SIM code to be executed by the processor in a protected manner to provide SIM capabilities without a discrete hardware SIM device, the SIM capabilities to be used to enable the wireless communications.

10. The computing system of claim 9 wherein the wireless communications are in accordance with one or more of the Global system for Mobile communications/General Packet Radio Services (GSM/GPRS), 3G, CDMA and Personal Handyphone System (PHS) protocols.

11. The computing system of claim 9 further comprising a hardware token.

12. The computing system of claim 11 wherein the hardware token is a Trusted Platform Module.

13. The computing system of claim 9 wherein the SIM code includes a provisioning module, the provisioning module, when executed, to communicate with a provisioning server over a trusted channel to provide for provisioning of SIM secrets.

14. The computing system of claim 13 wherein the provisioning module is to provide for protected storage of SIM secrets in an encrypted form on the computing system.

15. The computing system of claim 9 wherein the data store further stores encryption code to encrypt SIM secrets, the encrypted SIM secrets to be stored in the data store.

16. The computing system of claim 9 further including a Trusted Platform Module, the Trusted Platform to store a first key to be used by the encryption code to encrypt one or more of the SIM secrets and a second bulk encryption key used to encrypt the SIM secrets.

17. The computing system of claim 16 wherein the encryption code is to use the first Trusted Platform key to encrypt the second bulk encryption key and to store the encrypted second key in the data store.

18. The computing system of claim 9 wherein the data store is further to store a SIM Application Programming Interface (API).

19. The computing system of claim 18 wherein the SIM API provides access to at least one of a set of capabilities including

generation of authentication keys for use in a Authentication, Authorization and Accounting (AAA) mechanism, generation of encryption keys for encryption of data communications, access to user secrets, access to security policies, access to protected storage provided under a SIM file structure hierarchy, access to pre-configured SIM-based applications or utilities and access to provisioning capabilities.

20. The computing system of claim 9 wherein the SIM capabilities include capabilities associated with a Universal SIM (USIM) and the wireless communications are in accordance with a 3G network protocol.

21. A method comprising:

providing for wireless communications over a wireless network; and

providing AAA capabilities for the wireless communications without the use of a discrete SIM hardware device.

22. The method of claim 21 wherein providing for wireless communications over a wireless network includes providing wireless communications in accordance with one or more of GSM/GPRS, 3G network, CDMA, and PHS protocols.

23. The method of claim 21 wherein

providing AAA capabilities includes executing SIM code in a protected partition of a processor.

24. The method of claim 23 wherein

providing AAA capabilities includes executing SIM code under the control of an operating system that provides for protected execution of code.

25. The method of claim 24 wherein

executing SIM code includes selectively executing one or more of A3, A8 and A5 algorithms accessible by a computing system.

26. The method of claim 21 further comprising

encrypting SIM secret data, and

storing the encrypted secret data on a mass storage device of a computing system.

27. The method of claim 26 wherein,

encrypting SIM secret data includes using a bulk encryption key.

28. The method of claim 27 wherein

encrypting SIM secret data further includes encrypting the bulk encryption key using a second key provided by a Trusted Platform Module, and

storing the encrypted bulk encryption key on the mass storage device.

29. The method of claim 21 further comprising

provisioning one of SIM secret data and a SIM algorithm securely without the use of a discrete hardware SIM device.

30. The method of claim 29 wherein provisioning includes

executing a provisioning module,

establishing a protected communications link with a provisioning server, and

receiving one of the SIM secret data and the SIM algorithm from the provisioning server over the protected communications link.

31. A method comprising:

without the use of a discrete hardware SIM device,

establishing a first protected channel of communication with a provisioning server,

encrypting data to be sent from a computing system to the provisioning server, and

decrypting SIM secret data received by the computing system from the provisioning server.

32. The method of claim 31 further comprising:

establishing a second protected channel of communication to a network interface.

33. The method of claim 31 wherein, establishing the first protected channel of communication includes

generating a client key on the computing system using a hardware token,

providing the client key to the provisioning server, and

participating in a bilateral authentication routine with the provisioning server.

34. The method of claim 31 further comprising:

checking the integrity of the secret data.

35. The method of claim 34 wherein decrypting SIM secret data includes decrypting one of a unique client identity, a data object for initialization, a cryptography algorithm, a parameter update, an algorithm and a code update.

36. A method comprising:

receiving SIM secret data objects;

encrypting the SIM secret data objects in a protected execution environment provided by a computing system that does not include a discrete hardware SIM device using a bulk encryption key;

encrypting the bulk encryption key using a second key provided by a hardware token; and

storing the encrypted SIM secret data objects on a storage device in the computing system.

37. The method of claim 36 further comprising:

storing the encrypted bulk encryption key on the storage device.

38. The method of claim 36 wherein receiving SIM secret data objects includes receiving the SIM secret data objects over a protected channel.

39. A method comprising:

establishing a secure operating environment on a computing system that does not include a discrete hardware SIM device;

loading an encrypted SIM data object and associated encrypted first bulk encryption key into a protected memory;

receiving a second key from a hardware token in response to providing authorization data; and

decrypting the first bulk encryption key and the SIM data object.

40. The method of claim 39 wherein establishing the secure environment includes establishing a protected partition for protected execution.

41. The method of claim 39 wherein loading the encrypted SIM data object and associated encrypted first bulk encryption key includes loading the encrypted SIM data object and associated encrypted first bulk encryption key from a hard disk.

42. The method of claim 41 further comprising:

encrypting the SIM secret data with the first bulk encryption key after completing operations on the SIM secret data,

encrypting the first bulk encryption key with the second key,

binding the second key using the hardware token, and

storing the encrypted SIM secret data and encrypted first bulk encryption key on the hard disk.

43. A computer-accessible medium storing information that, when accessed by the computer system causes the computer system to:

provide an application programming interface to access at least one SIM capability from a set of SIM capabilities including generation of an authentication key, generation of an encryption key, access to user secret data, access to a security policy, access to protected storage provided under a SIM file structure hierarchy, access to SIM utilities, access to provisioning capabilities and access to SIM algorithms.

44. The computer-accessible medium of claim 43 wherein the SIM algorithms include at least one of an authentication, encryption and key generation algorithm.

45. The computer-accessible medium of claim 43 wherein the SIM algorithms include at least one of an A3, A8 and A5 algorithm.

46. A computer-accessible storage medium storing information that, when accessed by a computer system causes the computer system to:

execute an application program; and

access SIM capabilities provided by a computing system without a discrete hardware SIM device, the application program to access the SIM capabilities to provide one or more of authentication, authorization and accounting capabilities.

47. The computer-accessible storage medium of claim 46 wherein the application program is to access the SIM capabilities to provide authentication to a network.

48. The computer-accessible storage medium of claim 47 wherein the network is one of a wireless local area network, a wireless wide area network, and a wired network.

49. The computer-accessible storage medium of claim 46 wherein the application is to access the SIM capabilities to provide location-based services.